SOUTH CAROLINA DEPARTMENT OF DISABILITIES AND SPECIAL NEEDS

Volume 2, Issue 3

March 2003

Page 1 of 3

FROM THE DESK OF THE DDSN MEDICAL CONSULTANT

INSIDE THIS ISSUE:

Written by:

Graeme Johnson, M.D.

MEDICAL CONSULTANT

SCDDSN

3440 Harden Street Ext.

P.O. Box 4706

Columbia, SC 29240

PHONE:

(803) 898-9808

FAX:

(803) 898-9656

EMAIL:

gjohnson@ddsn.state.sc.us

EXTRANET:

http://web.ddsn.sc.gov/

PRIVACY AND HIPAA

When we care for our consumers we learn a great deal about them. This information is often very private, and we have a natural and professional responsibility to treat it with as much respect as the person to whom it belongs. We are particularly responsible for the privacy and confidentiality of facts that we learn during health care of a person. In recent years, concerns for protection of sensitive information led to many rules about privacy, being included in the 1996 federal Health Insurance Portability and Accountability Act known as HIPAA. There are several aspects of this act that we need to be aware of both in our work and in our personal dealings with any health care system.

PRIVACY RIGHTS

The privacy rules of HIPAA aim to give patients more control over their information. The rules limit the use and release of health records. The regulations establish safeguards that health care systems need to develop to protect the privacy of health information while accounting for the responsibility to the community, to allow some forms of information to be released to appropriate persons to protect public health. The rules also put in place civil and criminal penalties of fines and prison terms for serious violations of patient's privacy rights.

The original purpose of HIPAA was to allow us to have portability of health insurance, so that we can move the right to insurance without "preexistent condition" waiting clauses when we move from job to job. As most insurance transactions are electronic, there were related changes made to standardized data sets that were designed to increase the efficiency of the system. Along with this developed concerns about the privacy of the personal information in the system and in health care records as a whole, and its potential for use that was perhaps unknown by and even harmful to the patient. Therefore, the rules for privacy and security of information have developed. The privacy rules become effective April 14, 2003, and the final security regulations are yet to be advertised. The privacy rules apply to all health systems that use electronic transactions. South Carolina Department of Disabilities and Special Needs administers our state's medical funds for services for developmentally disabled persons, and it uses the electronic

PRIVACY RIGHTS (continued)

network. Therefore, all providers funded through SCDDSN will need to follow the rules. These regulations to a large degree are a formalization and enhancement of the policies that we have all used to protect privacy, and we need to take care to use the formal systems that protect confidential information.

WHAT DO WE NEED TO DO FOR HIPAA?

We are obligated to have clear privacy procedures and to have a designated person to mange them. We are all required to be trained in the procedures and understand how we are to follow them. We need to secure all patient records containing identifiable health information so that they are not easily available to persons who have no business to see them. We are responsible for restricting the release of information to the minimum needed for any purpose. The patient consent for treatment covers use of information for treatment, payment systems, and the operations of the health care provider. Consent for treatment will allow the sharing of information between professionals concerned with treatment. At all times information is only to be shared on a "need to know" basis.

The system needs to be able to tell patients about their privacy rights, how their information may be used and by whom, and for what purpose. Release of information for purposes other than treatment, payment or operations will require separate specific authorization from the patient. The patient has a right of access to their own health information at reasonable times and cost, and may request amendments to the records if necessary. The patient must be able to cancel the permission to disclose information to others at any time, and also have access to a formal complaint process if needed. As providers, we need to be careful to restrict the sharing of information. If outside agencies have access to our clients protected health information, then we need to have agreements that they follow privacy protection rules too. Any sharing of information beyond this will need release forms from the patient or their representative as defined in your agency's policies, and following SC and federal laws.

WHAT INFORMATION IS PROTECTED?

The information that we need to consider as protected health information includes personal facts like: **names, addresses, phone numbers, zip codes, email addresses, fax numbers, birthdays, social security numbers, family names and their addresses and phone numbers**. Clinical information would include: **pictures, notes of treatment, patient history, family histories, allergy information, laboratory and other test results, medication lists, dates of service and providers involved.**

This information can be used as needed within the treatment, payment, and operations system of the provider's agency without specific consent. However, outside of these areas, consent for release of information must be obtained. In all cases, any use or release of private medical information must be kept to the minimum necessary. We are able to give information to family members and other consumer representatives if the patients are not able to speak for themselves. Please check your agency's policies to see ways to follow this part of the rules.

WHAT ARE THE PRACTICAL THINGS WE NEED TO DO TO MEET HIPAA RULES?

As caregivers, we need to continue our positive care for our consumers. We need to be continuously watching how we follow current policies and be careful to improve our protection of privacy. Also, we have a little more documentation of information sharing to do – getting consent, recording with whom information shared, what was shared, and for what purpose if the sharing is outside our operations. We need to attend training and be aware of the policies and procedures we need to follow. Most of these are what we normally do, but sometimes we need to be a little more careful than we have been. We need to guard against passers-by overhearing confidential conversations in public places, even corridors or offices with open doors. We need to protect computer screens, notice boards and fax machine printout from easy reading by unauthorized staff or other persons. Written records should be secure and not easily read by the public. Any notes or papers with protected health information should be disposed of securely, preferably by shredding, but not left to blow away in the trash.

Privacy policies that your agency uses will include guidance on release of information to family, other agencies, law enforcement, etc. Please become aware of what these policies expect you to do. If in doubt, refer to your policies and ask for advice.

As a health care consumer yourself, you need to ask your provider about their privacy policy and read carefully all papers that you sign for your care. We need to respect the wishes of our consumers in the same way as we wish to be treated. Remember, the real test is "Would you like this information spread if it belonged to you?" HIPAA is largely a formal way to insist we consider this responsibility at all times.